

Digital credentials are a secure way to verify a person's identity in a computer system. Digital certificates and other online credentials, such as a driver's license or employee badge. Digital credentials can also verify a person's specific skills and accomplishments, such as completing a course or degree program. They are used by a variety of organizations, including businesses, nonprofits, educational institutions and training providers. In cybersecurity, digital credentials can help reduce the risk of identity-based cyberattacks. Threat actors today often find it easier to hijack valid accounts than to hack into a system. The IBM® X-Force Threat Intelligence Index found that the misuse of valid accounts is cybercriminals' most common entry point into victim environments, accounting for 30% of all incidents. Digital credentials can take the place of passwords and other authentication factors that hackers can easily crack. To take over an account, the attacker would need to steal the digital credential—which is much harder to do than brute-forcing a password. Digital credentials are often designed, created, delivered, managed and revoked by the issuing organization on an enterprise-grade digital credentials can verify a user's identity across multiple systems. Users can sometimes share their credentials manually through links, QR codes, digital files, apps and a blockchain. Digital credentials are available in multiple forms, specialized for different environments and functions. Common types include: Digital badges are often used as proof of a credentialsOpen BadgesDigital study. They can also be used as proof of identity or attendance at events and conferences. Digital badges usually take the form of a digital image or icon containing metadata such as the issuer's name, recipient's information, badge details are a type of digital badge used to verify smaller-scale accomplishments, such as completion of a webinar or individual modules in online courses. Microcredentials enable learners to focus on the specific modules of a larger course with the most valuable professional development or learning outcomes. Open Badges standard originally developed by the Mozilla Foundation. The standard supports badge interoperability across an ecosystem of websites and applications, including social media platforms such as LinkedIn and integrations with email signatures. such as by embedding it within an image. It also includes a mechanism for validating badges through cryptographic signatures. The term "digital certificate" can refer to two distinct kinds of credentials: those that verify a person's accomplishments and those that verify a person's accomplishment based digital certificates generally signify the same kinds of competencies as paper certificates, such as diplomas. One of the key differences between digital badges and certificates is that certificates is that certificates is that certificates are program at an educational institution, finishing a professional certificates are program at an educational institution. organization. Some types of digital certificates are used to identify and authenticate users, servers, services, computers, smartphones and Internet of Things (IoT) devices. These certificates are used to verify the holder's identity. Digital certificates use public key cryptography to authenticate certificates and prevent theft or forgery. Some organizations and credentials are not forged or stolen. Digital credentials stored on the blockchain cannot be altered and can be verified by anyone with access, which helps build trust among all stakeholders. The issuer—such as an educational institution or an enterprise security team—creates a digital credential are recorded on the blockchain. The holder stores their credential in a digital wallet. When the holder needs to verify their identity or some other assertion, they present the digital credential. The verifier—whoever needs to authenticate this holder—can check the credentials are not exactly a distinct type of credential, but an approach to creating secure, reliable credentials. Verifiable credentials are credentials that have some built-in way to be verified, such as a QR code that can be scanned to access verification information or a cryptographic signature from a trusted authority. Any of the other credential types listed here can be considered verifiable digital credentials as long as they meet this requirement. Some verifiable digital credentials adhere to the Verifiable Credentials standard from the World Wide Web Consortium. These credentials follow a structured approach for using JSON or JSON-LD to define characteristics such as issuer ID, holder attributes and cryptographic proof for authenticating the credential. insights on security, AI and more, weekly in the Think Newsletter. Authenticating professional credentials can facilitate verification processes in a variety of situations, including corporate, customer service and legal systems For example, with credentials on a smartphone app, an individual can prove their identity at airports, during traffic stops or when purchasing alcohol. New York State has launched just such a digital identity app in cooperation with the US Transportation (TSA).1 In the financial sector, digital credentials can strengthen and streamline identity verification for activities such as money transfers and account management. Tamper-proof credentials can be both more convenient and more reliable than passwords or other authentication factors, which can be forged or stolen. In government, digital credentials enable citizens to verify themselves so they can collect benefits and file taxes. Governments can trust that these citizens are who they say they are before releasing information or delivering services. Digital credentials can represent professional licenses and certifications, enabling individuals to easily prove their qualifications and competencies to potential employers. Credentials can validate nearly any assessment, credentialing program or professional learning experience, from coding boot camps to medical licenses. Higher-education institutions might also use them to validate degrees and diplomas. Less scrupulous job seekers have been known to fabricate achievements. Requiring verifiable digital credentials as proof can help employers spot them. Digital credentials can help facilitate data-sharing while complying with data privacy regulations such as the General Data Protection Regulation (GDPR) or the Health Insurance Portability Act (HIPAA). For example, some digital credentials allow for selective information sharing. Consider a digital credential in a healthcare setting, which might contain data about a patient's identity, insurance coverage without also disclosing their medical history. The same credential to confirm vaccine status or prescription history, too. In each scenario, only the necessary information is shared. Irrelevant data is kept private, which protects the credential holder and helps the organization comply with data privacy regulations. Credentials are often seen as a method for verifying the identity of a person, but they can also be used to authenticate physical assets and resources. For example, a company can use a blockchain to credential their products. Credentials can include information such as country of origin, product quality, regulatory compliance data and more. People and organizations can then use these blockchain-based credentials to verify the authenticity of products and combat counterfeiting. Improved identity and access managementStreamlined verificationImproved user experienceCredential longevity Verifiable digital credentials can help strengthen identity and access management (IAM) systems. IAM systems rely on authentication factors—such as passwords and security keys—to verify users' identities so they can receive the appropriate system access permissions. However, threat actors can steal or forge these factors with relative ease, allowing them to gain and abuse permissions they shouldn't have. Digital credentials offer an alternative. These credentials can be automatically shared and securely verified using cryptographic signatures, granting access to authorized users while detecting and blocking forged or stolen credentials. Digital credentials are integrated into existing systems and workflows, users do not have to remember anything or carry any special objects or devices. Instead, they can share digital credentials through APIs, links and QR codes, making authentication almost automatic. Artificial intelligence (AI) and machine learning (ML) can help speed identity verification even further—for example, by automatically cross-referencing credential data with trusted databases and looking for signs of tampering. Organizations can also outsource credential administration to a third-party service, such as Credly, for further time and cost savings. Digital credentials can also simplify customers can use digital credentials to authenticate themselves and gain access to their accounts. This more convenient process has the potential to encourage more user sign-ups. Customers are generally more willing to register with an organizations and educational institutions that grant credentials might cease operations, which can make it difficult to verify paper credentials such as diplomas. Digital credentials, however, can be independently authenticated—especially if they use decentralized methods such as a blockchain. They can remain usable and reliable long after issuing institutions have shut down. Digital transformation is a business strategy initiative that incorporates digital technology across all areas of an organization. It evaluates and modernizes an organization's processes, products, operations and technology stack to enable continual, rapid, customer-driven innovation. Today customers expect this ability from wherever they are, anytime they want, by using the device of their choice and with all the supporting information is to meet these expectations. Every organization's digital transformation is different. It can begin with a single focused technology project, or as a comprehensive enterprise-wide initiative. It can range from integrating digital technology and digital solutions into existing processes and products, to reinventing processes and products, to reinventing processes and products or creating entirely new revenue streams by using still-emerging technologies. But experts agree that digital transformation is as much about business transformation and change management as it is about replacing analog processes or modernizing existing IT. While often led by a company's chief information office (CIO), it requires the entire C-suite to align on new technologies and data-driven methodologies that can improve customer experience, empower employees and achieve business goals But, most importantly, companies should create a digital transformation framework and monitor improvements through tracking key performance indicators (KPIs) to see if the work produces results. The earliest, headline-making examples of digital transformation—Uber, AirBnB, Netflix—used mobile and cloud computing technologies to reimagine transactions and, sometimes, disrupt entire industries. The COVID-19 pandemic drove transformative innovations to better support remote and hybrid work. Today, organizations are applying artificial intelligence (AI), automation and other technologies to streamline workflows, personalize customer experiences, improve decision-making, and respond more quickly and effectively to market disruptions and new opportunities. Digital transformation can help companies increase customer loyalty, attract talented employees, foster competitive advantage and build business value. McKinsey research found that between 2018-2022, digital leaders achieved about 65% greater annual total shareholder returns than digital "laggards."1 Discover expertly curated insights and news on AI, cloud and more in the weekly Think Newsletter. In digital transformation, domains are essentially targets or levers for transformation. Most digital transformation are essentially targets and operating modelsProcessesProductsEmployee experienceCustomer experience Business model transformation is a fundamental change in the way that an organization delivers products, services and value to its customers, investors or stakeholders. Examples include: Delivering video through digital streaming, instead of physical disks (Netflix, Hulu) Enabling anyone with a car to make money driving, without purchasing a medallion (Uber, Lyft)Allowing customers to deposit checks without visiting the bank (mobile deposit) Organizations pursue business model transformation for any number of reasons—for example, to meet changing customer sto deposit) organizations pursue business model transformation for any number of reasons—for example, to meet changing customer sto deposit). in a highly competitive market. They might also see a chance to disrupt a market or industry in their favor with a new business model—or have a need to respond to a disruptive competitor. While business model—or have a need to respond to a disruptive competitor. optimization can include: Consolidating isolated or redundant workflows Creating intelligent workflows by using AIReplacing manual tasks with AI and automation Process optimization can help organizations lower costs, reduce waste (time, effort and materials), make better use of human capital, and help all stakeholders make smarter decisions faster. Organizations are incorporating digital innovation into their products, and into the way their products are developed, products that meet customer needs. Automobiles, for instance, are continually transformed in this way. Innovations range from the ability to view and operate a smartphone from a car dashboard, to sensors that prevent crashes and unintended lane changes, to vehicles that incorporate computer vision, geolocation, machine learning and robotic process automation (RPA) to operate with minimal or no human intervention. By implementing Internet of Things (IoT), operational technology and automation on the factory floor, manufacturers can speed production, reduce errors and defects and eliminate manual labor. By adopting agile or DevOps practices organizations can speed software development. Companies can also add value and competitive differentiation by offering technology alongside their existing services—witness the tracker apps offered by shipping companies and pizza vendors. Employee experience is a holistic approach to talent management that helps ensure that employees have the tools the need to succeed and thrive at work. also have a direct impact—positive or negative—on customer experience, business performance and brand reputation. Digital transformation efforts to improve employee benefits portals and internal communicationsProviding access to popular messaging and collaboration tools Supporting work from home (WFH) or remote work without sacrificing capabilities or productivity Enabling employees to connect securely to corporate resources with the devices and initiatives Customer experience, or CX, is the sum of customers' perceptions resulting from all their interactions with a business or brand—online, in-store and in day-to-day life. In the end, all digital transformation journeys lead to the customer experience domain. organizations. In the digital age, continually improving the customers expect to be able to do business anytime, anywhere and on any device-today customers depend on it. They plan their mornings knowing their phones tell them exactly how long it takes to drive to work, and their evenings knowing they can meet the food delivery driver at their door. They ignore customer service call center hours, knowing that they can download their bank and credit card history at tax time (or anytime). Customers count on these and scores of other digital innovations, and they are ready to count on new ones. Successful digital transformation positions organizations to anticipate and deliver the next innovations, and experiences customers will want. Virtually any digital transformation strategy, but these technology can play a role in an organization's digital transformation strategy. transformation initiatives. Cloud computing The original digital transformation enabler, cloud and private cloud infrastructure, combining orchestrated public cloud and private cloud resources from multiple vendors, provides the application portability, vendor flexibility and IT agility needed for enduring digital transformation initiatives, transformed existing business models (for example mobile tickets and wallets) and created entirely new ones (for example, Uber). Today customers insist on doing more business through mobile apps, whether simply ordering lunch or dinner from their favorite restaurant, or managing their banking and investments. Internet of Things (IoT) is the universe of devices equipped with sensors that collect and transmit data over the internet. IoT devices are where digital technology meets physical reality. Applications like supply chain logistics and self-driving cars generate real-time data that AI and big data analytics applications. Artificial intelligence (AI) and machine learning enable a computer or machine to mimic the capabilities and self-driving cars generate real-time data that AI and big data analytics applications. of the human mind. AI learns from examples, recognizes objects, makes decisions and quickly processes large tasks. Generative AI applications can answer customer service inquiries, deliver content on demand, and perform other activities automatically and without human intervention, freeing employees for higher-value work. AI also enables personalization on demand and at scale across marketing, customer service, sales and other areas of a business. Automation (RPA), to perform repetitive tasks such as bookkeeping, sending invoices, or looking up or archiving records. Unlike AI, which can learn from data and perform tasks more accurately over time, RPA is limited to following processes that have been defined by a user or programmer. DevOps and DevSecOps continuously integrates and automates security throughout the DevOps lifecycle, from planning through feedback and back to planning again. DevOps and DevSecOps practices provide the agile development foundation organizations need to respond with speed to market changes and innovate software continuously. Digitization is the conversion of paper-based information into digital data. It's also a cornerstone of foundational transformation initiatives in healthcare (electronic medical records or EMR), government (making public records more accessible and enabling citizens to make service requests online), and other industries. record of electronic transactions. Blockchain provides total transparency to those who require it and is inaccessible to those who don't. Organizations are using blockchain as a foundation for superresilient supply chains and cross-border financial services transformations. organizations can partner with each other to serve customers. The rise of business ecosystems, driven by APIs and other advanced technologies and a growing interconnectedness between noncompetitive companies. Software providers can enable users to sign in with accounts from third parties. For example, an email provider can create a marketplace where users can connect their task management software or customer relationship management (CRM) provider. Digital facsimiles of physical products or environments to test out ways to improve efficiency or effectiveness. For example, a manufacturer can make a digital twin of their shop floor to find ways to improve the location of machinery to increase output or reduce safety issues. Or a product manufacturer can create digital replicas of their products to identify ways to produce ones that are more ergonomic or easier to use. existing operations with trial-and-error improvements. Experts and organizations credit digital transformation with everything from improved supply chain and resource management to significant gains in overall productivity, profitability and competitive advantage. and loyalty Successful digital transformation can improve an organization's customer service through a chatbot, delivering personalized content in context during any logical transformation can improve and customer service through a chatbot, delivering personalized content in context during any logical transformation can improve and customer service through a chatbot, delivering personalized content in context during any logical transformation can improve and customer service through a chatbot, delivering personalized content in context during any logical transformation can improve and customer service through a chatbot, delivering personalized content in context during any logical transformation can improve and customer service through a chatbot of the customer service the customer service through a chatbot of the cu transaction—these are just some of the ways organizations can better satisfy and retain customers by using digital technology. Rapid, continually. Adoption of hybrid multicloud infrastructure provides access to the best digital tools and technologies as they emerge. Agile and DevOps practices enable developers to rapidly integrate these technologies into their applications and systems. Greater resilience to change The same flexibility and agility that enables rapid innovation also helps the organization respond faster to change in customer demand, new market opportunities and competitive threats. In its earliest days, digital transformation enabled upstarts to disrupt entire industries; today it also helps organizations create more streamlined workflows, processes and infrastructure as a result to disrupt entire industries; today it also helps organizations create more streamlined workflows, processes and infrastructure as a result to disrupt entire industries; today it also helps organizations create more streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the streamlined workflows, processes and infrastructure as a result of the stream strea of their transformations. Through automation and AI, organizations can cut down laborious menial tasks and free up their vital employees to spend more time with customers and other stakeholders. A more engaged workforce Digital transformation can improve employee engagement in any number of ways, from providing access to the latest tools and technologies to driving a culture of agile innovation in which employees are encouraged to experiment, take risk, 'fail fast' and learn continually. According to the latest Gallup Q12 meta-analysis, which evaluates the connection between employees are encouraged to experiment, take risk, 'fail fast' and learn continually. higher performance in everything from absenteeism to sales productivity and profitability.2 Stronger cybersecurity Digital transformation at risk. Adopting the latest security technologies can help an organization better detect and respond to threats, reduce successful attacks, and prevent or minimize any resulting damage. New revenue streams Infusion of the latest technologies into a company's IT portfolio can help create new opportunities for revenue, including revenue streams from websites, mobile apps, upselling through chatbots and more. AI and sophisticated metrics can help identity new product and service opportunities based on customers' website behaviors and buying patterns. And customers might simply be more inclined to purchase from companies like Netflix and Uber have disrupted their business models and ital transformation. But other organizations also have compelling stories about digital transformation initiatives that revolutionized their businesses. Here are just a few examples: Consumers have always known Audi for making beautiful, high-performance cars, but the company risked falling behind electric car upstarts as people wanted to move away from gas-powered cars. The German automaker not only wanted to enter the electric market in a significant way but also wanted to enter the electric market in a highly competitive marketplace driven by sustainability and convenience. Seeing the US' only tennis major in person is an amazing experience, but not every tennis fan could experience the tournament's hundreds of matches through the US Open app and website. The US Open used generative AI models to turn more than 7 million tournament data points into digital content that gave fans more context about the matching being played. The UK's system of public healthcare providers needed to balance providing more digital services to clients while maintaining a strong security posture. Its digital, data and technology delivery partner, NHS Digital, created a Cyber Security Operations Centre (CSOS) that is as a single point of coordination between NHS and external partners. It now monitors more than two billion malicious emails a year through targeted filtering. The independent German gas and oil company knew that AI would help it better harness data generated from across the organization. While several internal business and corporate units had begun using AI, it needed a centralized initiative to deploy it at scale. It started AI@Scale where projects incorporated scalability at the start. One such deployment automated data extraction from 2,000 PDF documents, freeing up employees to focus on more impactful work. The Korean manufacturing business conglomerate understood that even one successful cybersecurity attack might have devastating consequences. Its Doosan Digital Innovation (DDI) group consolidated multiple regional security operation centers (SOCs) to a unified, global SOC to streamline its security posture and deployed AI-based pattern matching. As a result, response times have decreased by about 85%. A digital twin is a virtual representation of an object or system designed to reflect a physical object accurately. It spans the object's lifecycle, is updated from real-time data and uses simulation, machine learning and reasoning to help make decisions. The studied object for example, a wind turbine, is outfitted with various sensors related to vital areas of functionality. These sensors produce data about different aspects of the physical object's performance, such as energy output, temperature, weather conditions and more. The processing system receives this information and actively applies it to the digital copy. After being provided with the relevant data, the digital model can be utilized to conduct various simulations, analyze performance problems and create potential enhancements. The ultimate objective is to obtain valuable knowledge that can be used to improve the original physical entity. Although simulations and digital twins both utilize digital models to replicate a system's various processes, a digital twin is actually a virtual environment, which makes it considerably richer for study. The difference between a digital twin can run any number of useful simulations to study multiple processes. The differences don't end there. For example, simulations usually don't benefit from having real-time data. But digital twins are designed around a two-way flow of information that occurs when object sensors provide relevant data to the system processor and then happens again when insights created by the processor are shared back with the original source object. By having better and constantly updated data related to a wide range of areas, combined with the added computing power that accompanies a virtual environment, digital twins can study more issues from far more vantage points than standard simulations can, with greater ultimate potential to improve products and processes. There are various types of digital twins is the area of application. It is common to have different types of digital twins co-exist within a system or process. Let's go through the types of digital twins to learn the differences and how they are applied. Component twins or Parts twins Component twins are the basic unit of a digital twin, the smallest example of a functioning component. Parts twins are troughly the same thing, but pertain to components of slightly less importance. what is known as an asset. Asset twins let you study the interaction of those components, creating a wealth of performance data that can be processed and then turned into actionable insights. System or Unit twins, which enable you to see how different assets come together to form an entire functioning system. System twins provide visibility regarding the interaction of assets and may suggest performance enhancements. Process twins, the macro level of magnification, reveal how systems work together to create an entire production facility. Are those systems all synchronized to operate at peak efficiency, or will delays in one system affect others? Process twins can help determine the precise timing schemes that ultimately influence overall effectiveness. The idea of digital twin technology was first voiced in 1991, with the publication of Mirror Worlds, by David Gelernter. with first applying the concept of digital twins to manufacturing in 2002 and formally announcing the digital twin as a means of studying a physical object can actually be witnessed much earlier. In fact, it can be rightfully said that NASA pioneered the use of digital twin technology during its space exploration missions of the 1960s, when each voyaging spacecraft was exactly replicated in an earthbound version that was used for study and simulation purposes by NASA personnel serving on flight crews. The use of digital twins enables more effective research and design of products, with an abundance of data created about likely performance outcomes. That information can lead to insights that help companies make needed product refinements before starting production, digital twins can help mirror and monitor production systems, with an eye to achieving and maintaining peak efficiency throughout the entire manufacturing process. Digital twins can even help manufacturers decide what to do with product lifecycle and need to receive final processing, through recycling or other measures. By using digital twins, they can determine which product materials can be harvested. While digital twins are prized for what they offer, their use isn't warranted for every manufacturer or every product created. Not is it worth it from a financial standpoint to invest significant resources in the creation of a digital twin. (Keep in mind that a digital twin is an exact replica of a physical object, which could make its creation costly.) Alternatively, numerous types of projects: Buildings, bridges and other complex structures are bound by strict rules of engineering. Mechanically complex projects: Jet turbines, automobiles and aircraft. Digital twins can help improve efficiency within complicated machinery and transmitting it. Manufacturing projects: Digital twins excel at helping streamline process efficiency, as you would find in industrial environments with co-functioning machine systems. Therefore, the industries that achieve the most tremendous success with digital twins are those involved with large-scale products or projects: Engineering (systems)Automobile manufacturingAircraft productionRailcar designBuilding constructionManufacturingPower utilities The rapidly expanding digital twins are already in use across many industries, the demand for digital twins are already in use across many industries, the demand for digital twins are already in use across many industries. twins lets owners and operators reduce equipment downtime while upping production. Discover a Service Lifecycle Management solution created by IBM® and Siemens. Digital twins are already extensively used in the following applications: Power-generation equipment Large engines, including jet engines, including jet engines and power-generation. turbines benefit tremendously from the use of digital twins, especially for helping to establish time frames for regularly needed maintenance. Structures and their systems Big physical structures, such as large buildings or offshore drilling platforms, can be improved through digital twins, particularly during their design. Also useful in designing the systems operating within those structures, such as HVAC systems. Manufacturing operations Since digital twins are meant to mirror a product's entire lifecycle, it's not surprising that digital twins have become ubiquitous in all stages of manufacturing, guiding products from design to finished product, and all steps in between. Healthcare services Just as products can be profiled by using digital twins, so can patients receiving healthcare services. The same type system of sensor-generated data can be used to track various health indicators and generate key insights. Automotive industry Cars represent many types of complex, co-functioning systems, and digital twins are used extensively in automotive industry Cars represent many types of complex. design, both to improve vehicle performance and increase the efficiency surrounding their production. Urban planning Civil engineers and others involved in urban planning Civil engineers and others involved in urban planning Civil engineers and others involved in urban planning activities are aided significantly by the use of digital twins, which can show 3D and 4D spatial data in real time and also incorporate augmented reality systems into built environments. A fundamental change to existing operating models is happening. A digital reinvention is occurring in asset-intensive industries that are changing operating models in a disruptive way, requiring an integrated physical plus digital view of assets. Digital twins are a vital part of that realignment. The future of digital twins is nearly limitless because increasing amounts of cognitive power are constantly learning new skills and capabilities, which means they can continue to generate the insights needed to make products better and processes more efficient. In this article on transforming asset operations with digital twins, learn how change impacts your industry. As the pace of digital transformation accelerates in the manufacturing and engineering industries, two concepts have gained significant traction: digital transformation accelerates in the manufacturing and engineering industry. purposes and offer companies unique advantages. Here, we will compare digital twins and digital twins and digital twin is a digital twins and behavior models. A digital twin is a digital twin is a digital twins and behavior models with all the design and operational data of the physical object, including geometry, performance data and behavior models with all the design and operational data of the physical object or system, complete with all the design and operational data of the physical object. The purpose of a digital twin is to simulate the behavior of equipment in real-time, allowing engineers and operators to monitor performance and identify system issues/anomalies. Digital twin technology uses Industrial Internet of Things (IIoT) sensors, machine learning and simulation software to collect product data and generate accurate models Teams can then use the models to predict maintenance needs, simulate changes to the system and optimize processes (e.g., safety protocols, reporting processes, etc.). For example, a digital twin of a wind turbine can simulate the impact of changing wind speed and direction on the turbine's performance, helping operators make informed decisions about maintenance and energy production. Discover expertly curated insights and news on AI, cloud and more in the weekly Think Newsletter. A digital thread is a digital thread is a digital thread insights and news on AI, cloud and more in the weekly Think Newsletter. aspects of the lifecycle. The purpose of a digital thread is to provide a complete and transparent view of manufacturing systems, enabling efficient collaboration and decision-making across all stages of the process. Digital threads use a variety of technologies, including computer-aided design (CAD) software, product lifecycle management (PLM) systems and Internet of Things (IoT) sensors, to collect and share data across workflows. Digital thread technology optimizes traceability, providing a way to track asset progress and ensure that all stakeholders are on the same page throughout the production process. For example, aerospace companies can create a digital thread to help assemble aircraft with digital engineering. Production teams utilize 3D-model-based systems to guarantee that aircraft are built exactly to engineering specifications and rely on the digital threads utilize virtual representations of real-world assets and processes, but they offer distinct capabilities. Digital twins are scalable, but only to a point. Digital twins to simulate entire digital environments, they are most useful in evaluating a specific production environment. A digital thread concept, on the other hand, is limitlessly scalable. Digital threads can connect to (almost) any other enterprise system, including digital twins. As such, digital thread technology may be best suited for operations and/or circumstances where data must be gathered from an array of departments, devices, systems and processes. On the contrary digital twins will better serve operations that rely primarily on repetitive machine processes within a specific production environment. Both digital threads enable teams to take data from digital twins and other sources and centralize the data flow across departments and production silos so that the entire company can access the same information. Data attached to a digital thread also tends to be more consistently accurate, because the automation features of a digital thread concept eliminate the need to manually transmit information between departments and workflows. Digital twins and digital threads help organizations increase system efficiency, reduce product design and limit system downtime. However, the impact of each technology will vary depending on manufacturer needs. Digital twins allow manufacturers to do the following:Engage in responsive monitoring in real timeConduct proactive risk assessments and utilize predictive troubleshooting for organizational assetsAccelerate innovation using digital mirroringDigital threads help manufacturers in the following ways:Build more agile operations by facilitating a continuous, synchronized data flowIncrease interdepartmental collaboration across assets and systemsOptimize connectivity between manufacturing and engineering processesStreamline product to market fasterEnsure regulatory compliance by tracking the entire product lifecycle, including design decisions, engineering changes and maintenance records Digital twins and digital threads are essential tools for companies looking to start or accelerate a digital transformation. Using advanced technological tools like IBM Maximo can help organizations get there optimize asset performance and streamline day-to-day operations. Using an integrated AI-powered, cloud-based platform, IBM Maximo offers comprehensive CMMS capabilities that produce advanced data analytics and support manufacturers looking to make informed decisions about system performance and optimization. Using IBM Maximo software, especially as a complement to existing enterprise resource management (ERP) systems or a manufacturing marketplace. A digital identity is a profile or set of information tied to a specific user, machine or other entity in an IT ecosystem. Digital IDs help computer systems distinguish between different users for access control, activity tracking, fraud detection and cyberattack prevention. In most systems, an entity's identity is made of their unique attributes. entities. For example, a human user's identity in a corporate network might include identity information such as their social media handles, Social Security number and network username. Verifiable digital identities are the foundation of authentication and authorization, the processes that IT systems use to verify users and grant them appropriate access. Both human and nonhuman users need digital identities to interact with digital services and one another. Trusted digital identities are who they say they are. Digital identities allow systems to monitor activity and determine which entities are taking which actions. Because of their importance to the digital identities are a major concern for organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security Alliance found that more than half of organizations (51%) see managing and security (51%) see managing (51%) see man and insights on security, AI and more, weekly in the Think Newsletter. There are multiple types of digital identities are the digital identities are the digital identities are the digital identities are the digital identities. Human digital identities are the digital identities are the digital identities are the digital identities. driver's license, Social Security number or biometric data such as fingerprints and facial recognition scans. Humans use their digital IDs to access digital resources, such as logging in to a bank account online or retrieving sensitive assets on a corporate network. Things (IoT) nodes and other devices. They often use unique identifiers such as certificates or tokens to authenticate and distinguish themselves. Just like a human user's digital ID, a machine's digital ID allows it to access certain digital resources, such as a business app fetching sensitive data from a cloud database. Federated identities enable individuals to use their digital identities across multiple systems and services. Federated identities are essentially a type of user or machine identity for each system. Interoperability—a standards-based approach to enabling different identity for each system. IT systems to exchange data—helps enable identity federation. Digital identities play a key role in the identity and access to digital resources. When a new user needs access to a system—a new employee on a company network o a new server in a data center—the user must establish a distinct digital identity in that system. The IAM system then uses these distinct digital asset, they must authenticate themselves with the IAM system. Authentication entails submitting some credentials—such as a username and password, date of birth or digital certificate—to prove the user is who they claim to be. For extra security, some IAM systems might use multifactor authentication (MFA), which requires users to provide more than one authentication factor to prove the user is who they claim to be. system checks the permissions associated with their unique digital identity and grants only those approved permissions. In this way, IAM systems keep out hackers while helping ensure that each individual user has the exact permissions. In this way, IAM systems keep out hackers while helping ensure that each individual user has the exact permissions. apps and online services. The SSO portal authenticates the user and generates a certificate or token that acts as a security key for various interconnected resources. Enhanced cybersecurity Digital identities help protect computer systems from threat actors, fraud, identity theft and other unauthorized activities. According to the X-Force Threat Intelligence Index, the theft of valid accounts is the most common way that cybercriminals break into victim environments, accounting for 30% of all incidents. Digital identities make it easier for organizations to track user activity. Not only can they distinguish between authorized users, but they can also spot suspicious behavior associated with authorized users' digital identities, which can signal an account takeover in progress. Extra measures, such as MFA and time-based credentials, can also help safeguard digital identities from being stolen or misused. These added layers of security can help drive revenue rather than drain budget. An IBM Institute for Business Value study found that 66% of operations executives view cybersecurity as a revenue enabler. Promoting trust Trust is key to enabling collaborative workflows among internal staff, customers, service providers and external partners. A strong digital identity management system helps users trust that the people, machines and services they connect with are authentic and reliable. Artificial intelligence (AI) can help speed up digital identity verification processes by analyzing huge datasets of digital identifiers, such as facial features, fingerprints or retina scans. This helps streamline and strengthen identity verification, further promoting trust within computer systems. Flexibility of location Part of the power of cloud services is that they can be accessed from almost anywhere. But strong identity verification processes are required to prevent unauthorized and fraudulent access. With the rise of remote work and cloud computing, users are increasingly distributed, and so are the resources that they need to access. A verified digital identity systems are increasingly distributed, and so are the resources that they need to access. A verified digital identity systems allow users to create their own portable digital identities and store them in digital wallets. Such ecosystems give identity control to the individual and take the onus of managing the identities, organizations can check their credentials against a shared trust registry. There is a vast array of use cases for digital identities across industries, with many supporting how users and applications interact with cloud resources. Governments often use digital identities enable citizens to verify themselves so they can collect benefits and file taxes, and governments can trust that these citizens are who they say they are. Digital identities enable patients to securely share health data with their providers, making it faster and easier to get multiple opinions before determining a medical treatment plan. Providers can use digital identity solutions to verify insurance coverage, monitor health devices and help comply with rules such as the Health Insurance Portability and Accountability Act (HIPAA). Digital identities enable sellers to deliver better customer experiences tailored to individual users based on their personal data. For example, digital identity systems enable customers to store payment data for later purchases, while retailers can use the order history associated with unique identifiers to generate personalized recommendations. Sign In or Register to comment. A content management system (CMS) is software that helps users create, manage, store, and modify their digital content. This all-encompassing system is a one-stop-shop to store content—such as apps, images, and websites—in a user friendly interface that is customizable to an organization's needs and their employees. It's also important to not confuse a CMS with digital asset management (DAM). The two systems complement one another but are not interchangeable. DAM software supports an organization by storing its digital assets in one centralized location. In other words, a CMS builds and manages the content for a brand's website, while a DAM is just the system to organize and store the brand's digital files. Get the weekly Think Newsletter for expert guidance on optimizing multicloud settings in the AI era. To understand how a content management system works, let's take a step back. A website that is manually run would require the individual or organization to code or write a static HTML file from scratch and upload it to the server for each web page. This requires significant time and energy and periodic updating that takes away precious resources from already busy organizations. A way to avoid this complex work is to use a CMS platform. The system is already created on the back-end and front-end, while all the creator sees is a user-friendly interface that allows them to make necessary changes in a simplified manner. The CMS is built to enhance the customer experience for web content that is viewed online or on a mobile app. Separately, the application programming interface, or APIs, are an important part of a successful CMS. APIs allow the system to connect across multiple domains. APIs for apps, phones, or websites can help ingest content from the CMS become authors within the system during the content creation stage and make updates to site content as much or as little as they'd like. The content updates can be previewed, reviewed, and approved within minutes. If there are updates that need to be seen across channels those changes can be saved for a later time. 2. Content is either scheduled to be published or can go live automatically. 3. The visitors of the website see the published content live and can continuously see updates as they are being made (if these changes are published). The first is a content management application (CMA), which is the part that allows the user to add and make changes to the website. It brings together HTML, CSS and JavaScript to deliver content that matches the organization's brand style. content delivery application (CDA). This takes the content input to the CMA and stores it behind the scenes, making it live and visible for all site visitors. These two parts work together so organizations no longer need to handle the best ways to market their products or offerings. The CMS is a vital software for those companies and organization has specific audio, image, or video file storage needs an enterprise management system (ECM) may be better suited. Small businesses looking to streamline their web design or ramp up their social media presence might benefit from a CMS. There is no coding knowledge necessary and the user interface is often easy enough for beginners. There are many different CMS options available. Each has its own purpose and relevant features to meet the organization's needs. Below are a few of the systems offered. WordPress: Originally was a web content management system that was built to publish blogs, but has extended into many other areas. The open source CMS is used by many companies around the globe to build and maintain their websites. The user interface is easily accessible and allows you to create and publish unlimited content. Squarespace: Unlike the CMSs mentioned above, Squarespace is an all-in-one content management system, meaning with a single subscription the owner can do it all without needing third-party integrations. This is a popular CMS for small businesses online and in-store. Joomla: This CMS is another open source system to built websites and online applications. It is SEO-friendly and features unlimited designs and built-in multilingual capabilities. businesses that want to create online stores. They are then able to edit and manage different content types through one software has a combination of CMS and DAM features. It's fitting for businesses looking for one platform to handle their content management digital asset management, digital enrollment, forms, and more. Salesforce CMS: This hybrid CMS allows organizations to create and deliver content to any device as the customer sees fit. The software is multi-language and can be run on the web or on an app. Wix: The web-based platform is software that creators and businesses use to make and manage their own websites without needing to know how to code. The platform provides advanced SEO features and marketing tools. A CMS offers a business, take a look at some 'must have' features. Since it is likely that an organization has multiple people to publish content, it's important to have publishing controls and permissions. Authors might have different roles and need varying levels of access to the CMS. Once those parameters are in place, the organization can establish a clear workflow for publishing content and other creative assets. The controls also prevent users or authors from publishing automatically and instead protects the organization. The last thing they want to do is struggle to upload said content. A CMS should have powerful content editing tools so that the upload process is simple. Some functions that users should be able to simply do in the CMS interface include adding images, videos, CTAs and outside forms. In addition, the CMS should have proper publishing tools or "drag-and-drop" features that make it easy to schedule and update content as needed. An organization's website is likely to change, more often than not because of a new product launch or a design refresh. But it may take several iterations for the organization to reach a final product that they like, in which case a staging tool is already in the CMS. This feature gives the ability to test out a new content design without having to make changes on their own terms. Ideally, the CMS system your organization chooses has a built-in analytics system to measure performance. Indicators like how visitors are interacting with the content and on which devices are among the important data points the CMS should maintain. If a CMS does not come with these analytics tool, such as Google Analytics. Some CMS may require a plug-in or third-party integration so that the analytics show up right on the users dashboard. The security of a site is extremely important, not only to the organization, but also to its employees and users who rely on it to store content and data. When choosing which CMS to use, check to see whether there are built-in security features and what security protocol the team must follow to adhere to the CMS standards. When seeking out a new CMS here are some good questions to have answered: - Does it have a web application firewall? - Is there a security team? - What is the cadence of static code analysis and vulnerability scans? - Does it come with a content delivery network (CDN) to help prevent DDoS attacks? When selecting a CMS for your organization, you must consider what theme offering works best for your goal and your brand. The particular needs for an e-commerce site vary greatly from a news organization publishing articles. The CMS that you end up choosing may provide different theme is accurate and optimized across all devices. The right CMS for your organization will be the one that best fits the needs of your users. Regardless of which type of CMS, or cloud-based—many of the benefits are consistent from one system to the next. Increased collaboration A CMS allows for cross-collaboration, especially when it comes to a content marketing team promoting certain content. With browser-based content management systems, users across the globe can access and collaborate on projects without the hassle of sending different versions of files to one another. User-friendly One of the best parts of a CMS is the ease of use and streamlined workflow. A user doesn't need to learn how to code or have any certain skill level to use the software. The CMS is user-friendly and accessible to anyone throughout an organization. Built-in SEO tools The importance of SEO has only increased over the years and that trend doesn't seem to be changing. A CMS typically provides built-in SEO features or plug-ins for optimizing content, simplifying what can feel like an overwhelming process and making it easy for the user. Highly scalable A CMS can grow with your business, whether it be a publication or an online store. The software can enhance web content management for editors and content creators in a way that helps organize a company, making scalability easier. Consistent branding A CMS can provide the tools that your organization needs for consistent branding on which CMS you choose, might offer even more features. Organization Over time, an organization might produce a mass amount of content. Being able to store it in an organized way is vital. Editorial organization is highly important as a business grows and ages. Users need specific permissions and scheduling functions, among other tools to make work streamlined. way that maintains its integrity and admissibility in court. Digital forensics is a field of forensic science. It is used to investigate cybercrimes but can also help with criminal and civil investigations. For instance, cybersecurity teams may use digital forensics to identify the cybercriminals behind a malware attack, while law enforcement agencies may use it to analyze data from the devices of a murder suspect. Digital forensics has broad applications because it treats digital evidence from a crime scene, digital forensics investigators follow a strict forensics processes to gather physical evidence from the devices of a murder suspect. when handling digital evidence to avoid tampering. Digital forensics and computer forensics are often referred to interchangeably. However, digital forensics involves gathering evidence specifically from computing devices, such as computers, tablets, mobile phones and devices with a CPU. Digital forensics and incident response (DFIR) is an emerging cybersecurity discipline that integrates computer forensics and incident response activities to accelerate the remediation of cyber threats while ensuring that any related digital evidence is not compromised. Stay ahead of threats with news and insights on security, AI and more, weekly in the Think Newsletter. Digital forensics, or digital forensics, or digital forensics, or digital forensics, or digital forensics solutions, weekly in the early 21st century that countries like the United States formalized their digital forensics, or dis provide forensics, or digital forensics, or standardization resulted from the rise of computer crimes in the 2000s and the nationwide decentralization of law enforcement agencies. With more crimes—officials needed procedures to ensure criminal investigations dealt with digital evidence in a way that was admissible in a court of law. Today, digital forensics is only becoming more relevant. To understand why, consider the overwhelming amount of digital data available on practically everyone and everything. As society continues to rely more on computer systems and cloud computing technologies, individuals continue to conduct more of their lives online across an ever-increasing number of devices, including mobile phones, tablets, IoT devices, and more. The result is more data—from more sources in more formats than ever before—that investigators can use as digital evidence to analyze and understand a growing range of criminal activity, including cyberattacks, data breaches, and criminal and civil investigations. Additionally, like all evidence, physical or digital, investigators and law enforcement agencies must collect, handle, analyze and store it correctly. Otherwise, data may be lost, tampered with or rendered inadmissible in court. Forensics experts are responsible for performing digital forensics investigations, and as demand for the field grows, so do the job opportunities. The Bureau of Labor Statistics estimates computer forensics job openings will increase 31 percent through 2029. The National Institute of Standards and Technology (NIST) outlines four steps in the digital forensic analysis process. Those steps include: Data collection Identify the digital devices or storage media containing data, metadata or other digital information relevant to the digital forensics investigation. For criminal cases, law enforcement agencies will seize the evidence from a potential crime scene to ensure a strict chain of custody. To preserve evidence integrity, forensics teams make a forensic duplicate of the data using a hard drive duplicator or forensic imaging tool. After the duplication process, they secure the original data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the investigators comb through data and conduct the rest of the invest data and con from various sources, including web browser histories, chat logs, remote storage devices, deleted space, accessible disk spaces, operating system caches and virtually any other part of a computerized system. Data analysis Forensic analysis Forensic analysis forensic tools to extract data and insights from digital evidence. For instance, to uncover "hidden" data or metadata, they might use specialized forensic techniques, like live analysis, which exposes data hidden using steganography (a method for concealing sensitive information within ordinary-looking messages). Investigators may also reference proprietary and open-source tools to link findings to specific threat actors. Reporting Once the investigation is over, forensic experts create a formal report that outlines their analysis, including what happened and who may be responsible. Reports vary by case. For cyber crimes, they might have recommendations for fixing vulnerabilities to prevent future cyberattacks. Reports are also frequently used to present digital forensics teams relied on live analysis, a notoriously tricky practice that posed a significant risk of tampering. By the late 1990s, the increased demand for digital evidence prompted the development of more sophisticated tools like EnCase and FTK, which allowed forensic analysts to examine copies of digital forensics tools. These tools can be hardware or software-based and analyze data sources without tampering with the data. Common examples include file analysis tools, which gather information from Windows-based computing systems that catalog user activity in registries. Certain providers also offer dedicated open-source tools for specific forensic purposes—with commercial platforms, like Encase and CAINE, offering comprehensive functions and reporting capabilities. CAINE, specifically, boasts an entire Linux distribution tailored to the needs of forensic teams. Digital forensics contains discrete branches based on the different sources of forensics include: Computer science and legal forensics: Investigating and evaluating digital evidence for computer science and other mobile devices. Database forensics: Examining and analyzing data found in computer network traffic, including web browsing and communications between devices. File system forensics: Examining data found in files and folders stored on endpoint devices like desktops, laptops, mobile phones, and servers. Memory forensics: Analyzing digital data found in a device's random access memory (RAM). When computer forensics and incident response—the detection and mitigation of cyberattacks in progress—are conducted independently, they can interfere with each other and negatively impact an organization. Incident response teams can alter or destroy digital evidence while removing a threat from the network. Forensic investigators can delay threat response into an integrated workflow that can help information security teams stop cyber threats faster while also preserving digital evidence that mitigation. Forensic data collection happening alongside threat mitigation: Incident responders use computer forensic techniques to collect and preserve data while they're containing and eradicating the threat, ensuring the proper chain of custody is followed and that valuable evidence isn't altered or destroyed. Post-incident review including examination of digital evidence isn't altered or destroyed. Post-incident review including examination of digital evidence isn't altered or destroyed. happened, the extent of the damage and how similar attacks can be avoided. DFIR can lead to faster threat mitigation, more robust threat recovery, and improved evidence for investigating criminal cases, cybercrimes, insurance claims and other security program with solutions from the largest enterprise security provider. Explore security services Artificial intelligence (AI) cybersecurity services and managed security services and managed security teams

with AI-powered cybersecurity solutions. Explore AI cybersecurity Whether you need data security, endpoint management or identity and access management or identity and access management (IAM) solutions, our experts are ready to work with you to achieve a strong security posture. Transform your business and manage risk with a global industry leader in cybersecurity consulting. cloud and managed security services. Explore cybersecurity solutions Discover cybersecurity services Digital transformation in banking is the act of integrating digital technologies and strategies to optimize operations and enhance personalized experiences. Across the financial services industry, this process can occur by breaking down data silos and reimagining the customer experience. The world is rapidly changing to be more digitally focused, especially in the banking industry. Traditional banks are undergoing major digital transformations in order to meet the needs of new customers and existing channels. To make it possible, banks and financial institutions must take on a digital transformation strategy that puts customer experience first by analyzing, interacting and understanding customer experience first by analyzing. banking sector, but it has become more relevant as fintech and new operating models have gained in popularity. Traditional banks must keep up with the changing market and ever-evolving customer needs, such as the drive toward using mobile apps or websites to perform transactions. These types of technology are part of the omnichannel strategy banks are using to break down data silos and reimagine the customer journey. With the more recent shift toward automation, banks must consider when creating a digital transformation strategy. Customers are seeking digital approaches to managing their accounts, prioritizing personalized product experiences, transparency and security—all in real-time. Mobile devices drive this digital transformation trend, along with customers increasing need to stay constantly connected. The only way to meet the customer needs is through a digital transformation journey. This journey harnesses customer data to analyze behavior patterns, enabling businesses to align more relevant products and services with their customers' needs. Customer journey: Considering the more customer-centric approach and by using data and other new technologies to tailor banking services to the individual customer. Modernized infrastructure: New technologies, such as automation and AI can streamline internal operations and ultimately boost efficiency and give these banks and financial service providers the competitive advantage. can have more informed and strategic decision-making. Breaking down these data silos provides more opportunity for better risk management and innovation. Security measures that better protect sensitive customer data. Online banking and digital services bring about a new layer of security concerns. With advanced technology in place, banks can bring in fraud detection measures and ensure that regulatory compliance is met. Digitization: The digital forward approach. For these reasons digital transformation initiatives are so important, such as partnering with fintech startups or open banking frameworks that aim to expand services for stakeholders. For a successful digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation to take place banks must take advantage of the latest digital transformation take place banks must take advantage of the latest digital transformation take place banks must take advantage of the latest digital transformation take place banks must take advantage of the latest digital transformation take banking and financial services sector. Application programming interfaces (APIs): An API is a software interface that allows for two or more software applications to integrate data services and partners? Furthermore, they can create new products and services for their customers and improve overall operational efficiency. Cloud computing resources, which banks and financial service providers have come to use and accept. The cloud environment allows for better operations and a more flexible infrastructure that's agile and scalable. AI and machine learning (ML): The AI and ML technologies are being used for several transformation efforts, including analyzing significant datasets, automating certain processes and improving the user experience through personalized services. AI in particular is used in banking through online assistants and chatbots that can address basic customer issues. Separately, an advantage of using ML in banking is that it makes it easier to track changes in user behavior and detect fraudulent activity faster. Internet of Things. (IoT): IoT refers to a network of physical devices, think wearable smartwatches or smart thermostats that are embedded with sensors and software that allows them to collect and share data. For banks, this smart connectivity has allowed customers to make instant contactless payments and interact with their accounts in a mobile banking capacity. The IoT can also be thanked for bringing risk management and advancements in the authorization process more than ever. Blockchain: The transparent and information-driven nature of blockchain makes it a trending technology for banks and financial service providers. It has resulted in more secure data transactions and an enhanced interface that meets and goes beyond customer expectations. Today, customers trust blockchain solutions and find it to be a more transparent way of operating business models. The changing market and push toward new technology make it imperative to evolve. While the digital transformation process can be intimidating, with the right resources and assistance, banks can see the tremendous benefits from the transformation journey. As your bank or financial service provider begins the transformation process, here are some basic steps to follow: Establish business and technical objectives and understand what they want to gain from the transformation item: Create a list of priority objectives to start and then tailor that list as the bank or financial institution leaders see fit. Evaluate your current technology Take stock of all the current systems has been made, evaluate them based on how each is working or not working toward your business goals. It's important to be transparent about your bank's process and be open to modifying it to fit the digital landscape. Action item: Be clear about your transformation, while also considering constraints including cost and timeline. Align scope and customer needs To understand what your clients need next, take back a step and evaluate how you're taking stock of current clients. Use data analysis to understand how you are segmenting and collecting data on clients. Use the data to understand which products are selling and which digital services are most popular to the clients. Use the data on clients are segmenting and collecting data on clients are selling and which digital services are most popular to the clients. more likely to use digital services. Ensure that your data is working for your business needs. Marketing teams can have a much more targeted approach once these consumers are identified and understood. Assess priorities Be realistic about your resources and what your organization can handle, in terms of both monetary and human resources. Define your target architecture and early proofs of value to measure achievements toward your business goals. Action item: Write out your objectives; list out ways in which you can enable your institution to make incremental changes at first. Early wins, even small ones, help with transformation buy-in and momentum. Present business case Once all transformation preparation has been made, present the business case for core systems transformation. Action item: Prepare your presentation for key stakeholders. Be prepared to defend the transformation needs you have found and laid out. Digitization in the banking system. The transformation process can bring about new opportunities for businesses of all sizes and bring forth banking solutions that provide greater customer-focused investment banking: Digital transformation in banking is more customer-focused than ever before. Because digital transformation in investment banking has replaced investment banks with small investors, the focus is now on short-term goals and all on one-digital platform. Offerings and technological decisions are now based on customer profiles. Easier compliance: By making the switch to a modern financial management system, banks and financial service providers can stay compliant. There are automated processes that can help employees allocate less time doing tasks like auditing reports and instead focus on the work that matters most. If a bank is on a cloud-based system, it provides timely updates and keeps up to date on regulations automatically. Access new clients: A digital-native environment makes attracting customers easier by being upfront about their services and what they can provide. By going digital, banks are making customer data. Thankfully, there are sophisticated software development services available to protect your customers personal information helps banks and financial institutions to hone in on exactly what a customer needs and wants. There is no longer the need to assume what a customer wants, with new technology, a bank can know exactly what it is the customer expects of them. Banking is no longer just a weekly practice, it's a daily act that requires a fast and secure ecosystem that customers can trust.